JOURNAL OF NUMBER THEORY 8, 58–72 (1976)

# G-Closed Fields and Imbeddings of Quadratic Number Fields

T. A. GADDIS

*Department of Mathematics, University of Arizona, Tucson, Arizona 85721*

*Communicated by O. Taussky-Todd*

Received May 25, 1973; revised February 25, 1975

A field, $K$, that has no extensions with Galois group isomorphic to $G$ is called $G$-closed. It is proved that a finite extension of $K$ admits an infinite number of nonisomorphic extensions with Galois group $G$. A trinomial of degree $n$ is exhibited with Galois group, the symmetric group of degree $n$, and with prescribed discriminant. This result is used to show that any quadratic extension of an $A_n$-closed field admits an extension with Galois group $A_n$.

## INTRODUCTION

Apply the square-root operator to an algebraic number field, $k$, until $k$ is closed with respect to the square-root operator. The resulting field, $K_0$, is said to be $C_2$-closed, where $C_2$ is the cyclic 2-group. We say $k_1$ is a $G$-extension of $k$ if $\mathrm{Gal}(k_1/k) \cong G$. Note that $K_0$ does not have a $C_2$-extension. In Section 1 this property is generalized to arbitrary finite groups, $G$; that is, to fields that do not have any $G$-extension. In Section 1.2, $G$-closed fields are shown to exist and be unique up to isomorphism. It is shown in Section 1.3 that there exists a finite extension, $L$, of a $G$-closed field that admits a $G$-extension; moreover, $L$ has an infinite number of $G$-extensions.

In Section 2 we consider the imbedding of quadratic number fields into fields with Galois group $S_n$, where $S_n$ is the symmetric group of degree $n$. This is accomplished by finding a trinomial with Galois group $S_n$ and prescribed square-free part of the discriminant. This result is used to show that for all $n \in \mathbb{Z}$, $n \neq 4$, an $A_n$-closed field has a quadratic extension, which in turn has an extension with Galois group $A_n$.

## 1. G-CLOSED FIELDS

### 1.1. *Definitions*

Let $K_0$ be the square-root field, that is the classical constructible numbers encountered in geometry. $K_0$ is the smallest field that contains $Q$, the rationals, and is closed under the square-root operation. Let $G_{K_0}$ be the set of all Galois groups of Galois extensions of $K_0$. There is no 2-group in $G_{K_0}$, although $K_0$ does have nonnormal extensions of degree $2^n$, $n > 1$. We generalize the above property of being closed under Galois extensions of degree two.

Throughout this paper $k$ will denote an arbitrary algebraic number field or a function field of transcendence degree one, $G$ will denote a finite group, and $C_n$ the cyclic group of order $n$.

We say that $k_1$ is a *G-extension* of $k$ if $\mathrm{Gal}(k_1/k) \cong G$. We define a *$G_t$-extension* of $k$ inductively:

(1) $k$ is a $G_t$-extension of $k$.

(2) If $k_1$ is a $G_t$-extension of $k$ and $k_2$ is the normal closure over $k$ of a $G$-extension of $k_1$, then $k_2$ is a $G_t$-extension of $k$.

(3) The union of a family $k_\alpha$, ordered by inclusion, of $G_t$-extensions of $k$ is a $G_t$-extension of $k$.

We define a field $K$ to be *G-closed* if it has no proper $G$-extensions.

We say a field $K$ is the *G-closure of $k$* if $K$ is a $G_t$-extension of $k$ and if $K$ is $G$-closed. It is assumed that $K$ is contained in an algebraically closed field, $\Omega$. The field of constructible numbers, $K_0$, mentioned above is the $C_2$-closure of $Q$.

### 1.2. *Properties of G-Closed Fields*

We now see that the $G$-closure of $k$ exists and is unique up to isomorphism.

PROPOSITION 1.1. *If $k$ is a field, then there exists an extension $K$ that is a $G_t$-extension of $k$ and is $G$-closed.*

*Proof.* Let $S$ be the set of all $G_t$-extensions of $k$. Note that $S$ is contained in $\Omega$. We now order $S$. If $F_1, F_2 \in S$, we write $F_1 \leqslant F_2$ if $F_1 \subseteq F_2$. $S$ is nonempty since $k \in S$, and is inductively ordered: If $\{F_i\}_{i \in I}$ is a totally ordered subset of $S$, then $\cup_{i \in I} F_i$ is an upper bound of $\{F_i\}_{i \in I}$. Therefore, by Zorn's lemma $S$ has a maximal element $K$, and $K$ is a $G_t$-extension of $k$. $K$ is $G$-closed, for if not there exists $K'$ such that $\mathrm{Gal}(K'/K) = G$ with $K' \in S$ and $K' \supset K$ contradicting the maximality of $K$.

PROPOSITION 1.2. *Let $k$ be a field, $E$ a $G_t$-extension of $k$ and $\sigma: k \to L$ an embedding of $k$ into a $G$-closed field $L$. Then there exists an extension of $\sigma$ to an embedding of $E$ in $L$. If $E$ is $G$-closed and $L$ is a $G_t$-extension of $\sigma k$, then any such extension of $\sigma$ is an isomorphism of $E$ onto $L$.*

*Proof.* Similar use of Zorn's lemma as in Proposition 1.1.

COROLLARY 1.3. *Let $k$ be a field, and $E$, $E'$ be the $G_t$-extensions of $k$. If $E$ and $E'$ are closed, then there exists an isomorphism $\tau: E \to E'$ inducing the identity of $k$.*

*Proof.* Extend the identity map on $k$ to an embedding of $E$ into $E'$ and apply Proposition 1.2.

As we saw above, the constructible numbers, $K_0$, are $G_2$-closed for $G_2$ a 2-group since by Sylow theory $G_2$ has a subgroup with index two. Moreover, $K_0$ is $G$-closed where $G$ is any finite group with a subgroup of index two. Extending to arbitrary $G$-closure, we have the following.

THEOREM 1.4. *If $K$ is the $G$-closure of $k$ and $H$ is a group extension of $N$ by $G$, then $K$ is $H$-closed.*

*Proof.* Assume $K$ is $G$-closed. If $K$ is not $H$-closed, then there exists an extension $L$ of $K$ with $\mathrm{Gal}(L/K) \cong H$. Since $N$ is normal in $H$, there exists by the fundamental theorem of Galois theory an extension $F$ of $K$ with $\mathrm{Gal}(F/K) \cong H/N \cong G$, thereby contradicting $K$ $G$-closed.

*Remark.* If $F$ is an algebraic field of characteristic $p \neq 0$, then $F$ is what Gordon and Straus [2] call a *CE* field; i.e., a field in which all finite extensions $E/F$ are cyclic. In [2] they prove the following theorem: $F$ is a *CE* field if and only if for each $n \in N$, the natural numbers, $F$ has at most one separable extension of degree $n$. For $F$ a *CE* field the $G$-closure of $F$ is closed under cyclic extensions of $G$, and under all subgroups of $G$.

A property similar to the $G$-closure of $k$ is the hull closure of $k$. A hull of groups as defined by Krakowski [6] is a set of groups $P$ closed under the operations of group extension and homomorphic images. A finite or infinite Galois extension $K$ of $k$ is called a $P$-extension when $\mathrm{Gal}(K/k)$ is in $P$. The $P$-closure of $k$ is the maximal $P$-extension of $k$. Note that $G$-closed is not the same as $P$-closed since a $G$-closed field may not be closed under homomorphic images of $G$. This happens in the case of the $C_4$-closure of $Q$ having $(-1)^{1/2}$ as a $C_2$-extension.

### 1.3. "*Opening Up*" *G-Closed Fields*

The above theorems describe the way in which the $G$-closure of $k$ is closed. Now we see how to "open up" a $G$-closed field. In order to do this we need the following lemma and theorem.

LEMMA 1.5. *For any distinct primes $p$, $q$, with $q$ odd, there is a solvable group $G$ of order $qp^{q-1}$ with subgroups $H$ and $H_1$ such that $H_1 \lhd H \lhd G$ with $(G : H) = q$ and $(H : H_1) = p$. Furthermore, $G$ does not have a normal subgroup, $H_0$, with index $p$.*

*Proof.* Let $H$ be the direct product of $q - 1$ copies of $C_p$, with $c_i$ $i = 1,..., q - 1$ the generators of the cyclic components of $H$; also let $H_1$ be the product of $q - 2$ of the above factors. Now aut$(H)$ has an element, $x$, of order $q$; namely:

$$x\colon c_i \to c_{i+1}, \qquad i = 1,..., q - 2,$$

$$x\colon c_{q-1} \to c_1^{-1}c_2^{-1} \cdots c_{q-1}^{-1}.$$

Thus let $G$ be the semidirect product of $H$ and $C_q$, $G \times H \mathbin{\mathbf{X}}_s C_q$, where $x$ generates $C_q$ and acts on $H$ as an inner automorphism. Clearly, $G$ is solvable with $H_1 \lhd H \lhd G$ and corresponding indices $p$ and $q$. To show that $G$ has no normal subgroup, $H_0$, of index $p$ it suffices to show that the commutator subgroup, $G'$, of $G$ is equal to $H$. Note that

$$[x, c_i] = xc_ix^{-1}c_i^{-1} = c_{i+1}c_i^{-1}, \qquad i = 1,..., q - 2,$$

$$[x, c_{q-1}] = xc_{q-1}x^{-1}c_{q-1}^{-1} = c_1^{-1}c_2^{-1} \cdots c_{q-2}^{-1}c_{q-1}^{-2}.$$

Since an arbitrary element of $G$ is of the form $hx^n$, $h \in H$, an arbitrary element of $G'$ is of the form $[h_1x^{n_1}, h_2x^{n_2}] = \prod[x, c_i]$ because $x^nc_i = c_{i+n}x^n$. Thus $G'$ is generated by $[x, c_i]$ $i = 1,..., q - 1$, which are independent and hence also generate $H$; so $G' = H$. Now if there did exist an $H_0 \lhd G$ such that $G/H_0 = C_p$, then $H_0 \supset G'$.

Therefore $(G : H_0)(H_0 : G') = (G : G') = q$, which is impossible since $(G : H_0) = p$ and $p \neq q$.

THEOREM 1.6. *Given a prime $p$ and an $n \in N$ such that $p \nmid n$, then there exists a solvable group $G_s$ such that $H_1 \lhd H \lhd G_s$ with $(G_s : H) = n$, $(H : H_1) = p$ and there does not exist a subgroup $H_0 \lhd G_s$ with $(G_s : H_0) = p$.*

*Proof.* Let $q$ be a prime dividing $n$, so $n = qs$; and let $S$ be a solvable group of order $s$. Let $G$ be the group as in Lemma 1.5. Taking $G_s$ to be the direct product of $G$ and $S$, we then have $G_s$ solvable with $H_1 \lhd H \lhd G_s$ and with the desired indices. Also, if $G_s$ did have $C_p$ as a homomorphic image, $S$ would have to be mapped onto the identity of $C_p$ since $p \nmid s$. Thus $G$ would have $C_p$ as a homomorphic image, which contradicts $G$ not having a subgroup of index $p$.

*Remark.* Since $G_s$ is solvable, it is a Galois group over $k$ by a result

of Šafarevič [9]. Take $H$, $H_1$, and $G_s$ as in Theorem 1.6. Let $M$ be an extension of $k$ with Galois group $G_s$, let $L_1$ belong to $H_1$, and let $L$ belong to $H$; thus we have

$$1 \lhd H_1 \lhd H \lhd G_s, \qquad k \subset L \subset L_1 \subset M,$$

with $\mathrm{Gal}(L/K) \cong G_s/H$ and $\mathrm{Gal}(L_1/L) \cong H/H_1 \cong C_p$. In the next theorem we show that the above tower of fields exists when the base field is $C_p$-closed.

We will need the definition of linearly disjoint for the proof of Theorem 1.7. Let $L$ and $K$ be two algebraic extensions of $k$; and let all fields involved be contained in $\Omega$, algebraically closed. We say that $K$ is linearly disjoint from $L$ over $k$ if every finite set of elements of $K$ that is linearly independent over $k$ is still independent over $L$.

THEOREM 1.7. *Let $K$ be the $C_p$-closure of $k$, and $n \in N$ be such that $p \nmid n$, then $K$ has a Galois extension $L'$ with $[L' : K] = n$ and $L'$ has a Galois extension $L_1'$ with $\mathrm{Gal}(L_1'/L') \cong C_p$.*

*Proof.* Let $L$, $L_1$, $M$, and $G_s = \mathrm{Gal}(M/k)$ be as in the remark above. Since $G_s$ has no subgroups of index $p$, $M$ and $K$ are linearly disjoint over $k$; moreover $L$ and $L_1$ are linearly disjoint with $K$. Taking composites we have

$$K \subset KL \subset KL_1 \subset KM$$

with $\mathrm{Gal}(KL/K) \cong G_s/H$, which has order $n$, and $\mathrm{Gal}(KL_1/KL) \cong C_p$. Letting $L' = KL$ and $L_1' = KL_1$, we have the desired extensions of $K$.

The above theorem has the following immediate corollary.

COROLLARY 1.8. *Let $L'$ be as in Theorem* 1.7 *and $p$ an odd prime; then the $C_p$-closure of $L'$ is a $(C_p)_t$-extension of $L'$.*

*Notation.* Let $\bar{k}_{C_p}$ denote the $C_p$-closure of $k$.

THEOREM 1.9. *Let $\{q_1, q_2, \ldots\}$ be an infinite sequence of distinct primes none of which is equal to $p$, an odd prime; then we have the following chain of fields:*

$$k \subset \bar{k}_{C_p} \subset K_1 \subset \bar{K}_{1C_p} \subset K_2 \subset \bar{K}_{2C_p} \subset \cdots \subset K_i \subset \bar{K}_{iC_p} \subset K_{i+1} \subset \cdots,$$

*where $[K_1 : \bar{k}_{C_p}] = q_1$ and $[K_{i+1} : \bar{K}_{iC_p}] = q_{i+1}$, $i = 1, 2, \ldots$.*

*Proof.* Induction on $i$: $i = 1$ is Theorem 1.7 with $n = q_1$ and Corollary 1.8. Assume true for $i = j$. By Theorem 1.7 $\bar{K}_{jC_p}$ has an extension

$K_{j+1}$ with $[K_{j+1} : \overline{K}_{jC_p}] = q_{j+1}$ since $q_{j+1}$ is relatively prime to all the $q_k$ $k < j+1$, and $p$. Furthermore, by Theorem 1.7 $K_{j+1}$ has a $C_p$-extension, and hence by Corollary 1.8 $\overline{K}_{j+1C_p}$ is a $(C_p)_t$-extension of $K_{j+1}$.

It has been shown that after an extension of degree $n$, $p \nmid n$, a $C_p$-closed field has at least one $C_p$-extension. We will now give an explicit extension of degree three of the constructible numbers that has an infinite number of $C_2$-extensions. Hilbert's irreducibility theorem will be needed to prove this result.

HILBERT'S IRREDUCIBILITY THEOREM 1.10. *Let $k$ be an algebraic number field, and $f(t_1,..., t_r, x_1,..., x_s)$ a polynomial with coefficients in $k$, which is irreducible as a polynomial in $r+s$ variables. Then there exists an infinite number of values $(t_1',..., t_r')$ of $(t_1,..., t_r)$ in $k$ such that the polynomial $f(t_1',..., t_r', x_1,..., x_s)$ is irreducible as a polynomial in $(x_1,..., x_s)$ with coefficients in $k$.*

*Proof.* See [7, p. 141].

*Remark.* If $K$ is the $C_2$-closure of $k$, then every cubic extension of $K$ is of the form $q^{1/3}$ with $q \in K$, but $q^{1/3} \notin K$. This follows since the discriminant of every cubic over $K$ is a square in $K$, and $\omega = (-1 + (-3)^{1/2})/2$ is in $K$.

THEOREM 1.11. *If $K$ is the $C_2$-closure of $k$ and $q \in K$ is not a cube, then $K(q^{1/3})$ has an extension $L$ with* $\mathrm{Gal}(L/K(q^{1/3})) \cong C_2$.

*Proof.* Let $f(x) \in K[x]$ be the polynomial belonging to $q^{1/3}$, i.e. $f(x) = x^3 - q$. Let $F = k(q, \omega)$ and $\widetilde{F(y)}$ be the algebraic closure of $F(y)$. Claim: There are infinitely many $a \in K$ for which $(q^{1/3} - a)^{1/2} \notin K(q^{1/3})$.

*Note.* $(q^{1/3} - a)^{1/2}$ belongs to $f(x^2 + a)$. Thus $(q^{1/3} - a)^{1/2} \in K(q^{1/3})$ if and only if $f(x^2 + a) = -g_a(x)\, g_a(-x)$, where $g_a(x) \in K[x]$.

Now let $a$ be a transcendental, say, $y$. Consider the factorization: $f(x^2 + y) = (x^2 + y)^3 - q = x^6 + 3yx^4 + 3y^2x^2 - q + y^3 = [x^3 + A(y)\, x^2 + B(y)\, x + C(y)][x^3 - A(y)\, x^2 + B(y)\, x - C(y)]$, where $A(y), B(y), C(y) \in \widetilde{F(y)}$.

We now determine the Galois group of $B(y)$.

Equating coefficients we have

$$3y = 2B - A^2,$$

$$3y^2 = B^2 - 2AC,$$

$$y^3 - q = -C^2,$$

which implies $A = (B^2 - 3y^2)/2C = (2B - 3y)^{1/2}$. Therefore we must solve

$$B^4 - 6y^2B^2 + 9y^4 - 4C^2(2B - 3y) = 0 \tag{1.1}$$

or

$$B^4 - 6y^2B^2 + 8(y^3 - q)B - 3y(y^3 - 4q) = 0. \tag{1.2}$$

Note that (1.2) is a polynomial equation over $F(y)$. We use Lagrange's method, see [14, pp. 272–275], to solve (1.2). The cubic resolvent of (1.2) is

$$w^3 + 6y^2w^2 + 12y(y^3 - 4q)w + 2^3y^6 - 2^5 \cdot 5qy^3 - 2^6q^2 = 0, \tag{1.3}$$

while the resolvent of (1.3) is

$$T^2 - 2^6 \cdot 3^3q(y^3 + q)T + 2^{12} \cdot 3^6q^3y^3 = 0. \tag{1.4}$$

Equation (1.4) has roots $t_1 = 2^6 \cdot 3^3qy^3$ and $t_2 = 2^6 \cdot 3^3q^2$.

Thus (1.3) has roots $w_1 = -2y^2 + 4q^{1/3}y + 4q^{2/3}$, $w_2 = -2y^2 + 4\omega^2q^{1/3}y + 4\omega q^{2/3}$, $w_3 = -2y^2 + 4\omega q^{1/3}y + 4\omega^2q^{2/3}$.

Therefore the degree of the splitting field of (1.3) over $F(y)$ is three. Hence by a well-known theorem (see [5, p. 52]), Equation (1.2) has Galois group $A_4$, or has a root in $F(y)$. But by Gauss' lemma, (1.2) does not have a root in $F(y)$. By Hilbert's irreduciblity theorem there are an infinite $n \in N$ so that $A_4$ is the Galois group of $B(n)$ over $F$. Since $A_4$ has no subgroup of index two, the Galois group of $B(n)$ over $K$ is $A_4$. Thus there are an infinite number of $a \in K$ so that $f(x^2 + a)$ does not factor in $K[x]$.

COROLLARY 1.12. *Let $K(q^{1/3})$ be as in Theorem* 1.11; *then the $C_2$-closure of $K(q^{1/3})$ is an infinite extension of $K(q^{1/3})$.*

*Proof.* If $(q^{1/3} - a)^{1/2^n} \in K((q^{1/3} - a)^{1/2^{n-1}})$ for $n$ finite, then $(q^{1/3} - a)^{1/2}$ would be in $K(q^{1/3})$, contradicting the theorem. Also, if $(a_1, a_2) = 1$ and $(q^{1/3} - a_i)^{1/2} \notin K(q^{1/3})$ for $i = 1, 2$, then $(q^{1/3} - a_1)^{1/2}$ and $(q^{1/3} - a_2)^{1/2}$ give rise to disjoint $C_2$-extensions of $K(q^{1/3})$.

## 2. THE IMBEDDING PROBLEM FOR QUADRATIC FIELDS

In 1892 Hilbert [4] showed, using his irreducibility theorem, that there exists a polynomial $f(x)$ with Galois group $S_n$, the symmetric group of degree $n$. We will give for all $n \geqslant 3$, $n \in N$ a polynomial $f(x)$ of degree $n$ that has Galois group $S_n$ and has prescribed square-free part of the discriminant. This is a particular solution of the imbedding problem.

In the general case the imbedding problem is one in which a Galois extension $F/k$ is given, and it is required to extend $F/k$ to an extension $K/k$ so that $\mathrm{Gal}(K/k)$ is a given group extension of a group $N$ by $\mathrm{Gal}(F/k)$. For $N$ abelian see [10], and for $N$ characteristically simple see [11].

We will need several lemmas to prove our main result.

Let $d$ in $k$ be such that the ideal $(d)$ is not a square. Note that for every prime ideal $\mathfrak{p}$ there is a $d_1 \sim d$ ($d_1 \in dk^{*2} \cap \mathcal{O}_k$) so that either $\mathfrak{p} \mid d_1$ if $(d)$ is divisible by an odd power of $\mathfrak{p}$ or $\mathfrak{p} \nmid d_1$ if $(d)$ is divisible by an even power of $\mathfrak{p}$. By $d$ square-free in $k$ we will mean $d$ or $d_1 \sim d$ such that the above property holds in $k$.

LEMMA 2.1. *Let $d$ be square-free in $k$; then $a$ and $b$ can be chosen in $k$ so that the discriminant, $D(f)$ of $f(x) = x^n + ax + b$ is equal to $dm^2$, $m \in \mathcal{O}_k$, $\mathcal{O}_k$ the integers of $k$.*

*Proof.* See [12] for a derivation of

$$D(f) = (-1)^{[n(n-1)/2]+n+1}(n-1)^{n-1}a^n + (-1)^{n(n-1)/2}n^n b^{n-1}.$$

Now if we prescribe the discriminant of $f$ to be $dm^2$, we can solve for $a$ and $b$ in terms of $d$. To do this consider the following cases:

*Case* 1. $n$ is odd. Let $b = (n-1)ar/n$, $m = s((n-1)a)^{(n-1)/2}$ where $r$, $s$ are arbitrary integers in $k$. Thus

$$D(f) = (-1)^{[n(n-1)/2]+(n+1)}(n-1)^{n-1}a^n + (-1)^{n(n-1)/2}n(n-1)^{n-1}a^{n-1}r^{n-1} = (n-1)^{n-1}a^{n-1}s^2d.$$

Therefore

$$a = -nr^{n-1} + (-1)^{n(n-1)/2}s^2d$$

and

$$b = -n^{-1}(n-1)r[(nr^{n-1} - (-1)^{n(n-1)/2}s^2d].$$

Hence

$$f(x) = x^n - [nr^{n-1} - (-1)^{n(n-1)/2}s^2d]x - [r(n-1)n^{-1}][nr^{n-1} - (-1)^{n(n-1)/2}s^2d]. \tag{2.1}$$

*Case* 2. $n$ is even. With $b = (n-1)ar/n$, $m = s((n-1)a)^{n/2}$ where $r$, $s$ are again arbitrary integers in $k$, we obtain in a similar manner:

$$f(x) = x^n + nr^{n-1}[1 + (-1)^{n(n-1)/2}(n-1)s^2d]^{-1}x + (n-1)r^n[1 + (-1)^{n(n-1)/2}(n-1)s^2d]^{-1}. \tag{2.2}$$

In what follows let $k$ be an algebraic number field with $\mathfrak{p}$ a prime ideal in $k$, where $\mathfrak{p} \cap \mathbb{Z} = (p)$ and $k_{\mathfrak{p}}$ is the associated valuated field.

THEOREM 2.2 (Eisenstein irreducibility criterion). *Let* $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in k_{\mathfrak{p}}[x]$. *Assume that* ord $a_i \geqslant 1$ *for* $i = 1,\ldots, n-1$ *and* ord $a_n = 1$. *Then* $f(x)$ *is irreducible in* $k_{\mathfrak{p}}[x]$.

*Proof.* See [8, p. 113].

LEMMA 2.3. *Let* $f(x)$ *be as in* (2.1) *or* (2.2) *of Lemma* 2.1; *then in either case* $r$, $s$ *can be chosen so that* $f(x)$ *is irreducible, over* $k$.

*Proof.* Let $f(x)$ be as in 2.1 and $p_1'$ a prime such that $p_1' \nmid n(n-1)$. Let $\mathfrak{p}_1'$ be a prime ideal in $k$ containing $(p_1')$. With proper choice of $p_1'$, we have $d \notin \mathfrak{p}_1'$. Now pick $r$, $s \notin \mathfrak{p}_1'$ so that $\operatorname{ord}[nr^{n-1} - (-1)^{n(n-1)/2}s^2d] = 1$. Thus $\operatorname{ord}\{[(n-1)rn^{-1}][nr^{n-1} - (-1)^{n(n-1)/2}s^2d]\} = 1$. Therefore $f(x)$ is irreducible in $k_{\mathfrak{p}_1'}[x]$ by Theorem 2.2. Hence $f(x)$ is irreducible in $k[x]$.

By Theorem 2.2 the polynomial (2.2) is irreducible or has a root in $k$. The reciprocal polynomial is of the form: $(n-1)y^n + ny^{n-1} + c = 0$, where $c = 1 + (-1)^{n(n-1)/2}(n-1)s^2d$ and $y = r/x$. Thus we have

$$1 + (-1)^{n(n-1)/2}(n-1)s^2d = c = -[(n-1)y^n + ny^{n-1}],$$
$$(n-1)y \in \mathcal{O}_k.$$

Now let $s$ run through the congruence class mod $p_1$, $p_1$ prime in $k$. Hence the left-hand side of the above equality has density proportional to that of all squares, while the right-hand side has density proportional to that of all $n$th powers, with $n > 2$. Thus the right-hand side has lower density than the left-hand side. Therefore we can choose $s$ so that the above equality does not hold, and consequently polynomial (2.2) does not have a root.

In 1922 Furtwängler [1] proved a theorem, giving conditions on a polynomial in $Q[x]$ so that it has primitive Galois group over $Q$. (For definition of primitive group, see [3, p. 64].) This theorem is easily extended to $k$.

THEOREM 2.4. *Let* $h(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathcal{O}_k[x]$, *irreducible and assume* ord $a_i \geqslant 1$ *for* $i = 1, 2,\ldots, n-2$, ord $a_{n-1} = 1$ *and* ord $a_n \geqslant 2$; *then* $h(x)$ *has primitive Galois group.*

LEMMA 2.5. *Let* $f(x)$ *be as in* (2.1) *or* (2.2) *of Lemma* 2.1; *then in either case* $r$ *and* $s$ *can be explicitly chosen so that* $f(x)$ *has primitive Galois group over* $k$.

*Proof.* Recall that for every prime ideal $\mathfrak{p}$ there is a $d_1 \sim d$ ($d_1 \in dk^{*2} \cap \mathcal{O}_k$) so that either $\mathfrak{p} \| d_1$ if $(d)$ is divisible by an odd power of $\mathfrak{p}$ or $\mathfrak{p} \nmid d_1$ if $(d)$ is divisible by an even power of $\mathfrak{p}$.

Now let $f(x)$ be as in (2.1), and since $d$ is assumed to be square-free, we may choose a prime ideal $\mathfrak{p}_2'$ so that $\mathfrak{p}_2' \| d_1$ and $d_1 \sim d$. Also, choose $r$, $s$ so that $r \in \mathfrak{p}_2'$ and $s \in \mathfrak{p}_2'$. Let $p_2'$ be the rational prime so that $(p_2') = \mathfrak{p}_2' \cap \mathbb{Z}$. If $p_2' \mid n$, then for some $\nu$ we have $(p_2')^\nu \| n$; in this case let $r \in (\mathfrak{p}_2')^{\nu+1}$. Now $\operatorname{ord}[nr^{n-1} - (-1)^{n(n-1)/2} s^2 d] = 1$, and

$$\operatorname{ord}\{[(n-1) rn^{-1}][nr^{n-1} - (-1)^{n(n-1)/2} s^2 d]\} \geqslant 2.$$

Therefore by Theorem 2.4 $f(x)$ has primitive Galois group.

Now let $f(x)$ be as in (2.2), and pick $\mathfrak{p}_2$ unramified in $k$ with $\mathfrak{p}_2 \cap \mathbb{Z} = (p_2)$ so that $p_2 \nmid n(n-1)$ and $d \notin \mathfrak{p}_2$. Choose $r$, $s \in \mathbb{Z}$ such that $p_2 \| r$, and $[1 + (-1)^{n(n-1)/2} (n-1) s^2 d] \equiv 0 \bmod p_2^{n-2}$. That is, $s$ is a solution to the following: $s^2 \equiv \pm d^{-1}(n-1)^{-1} \equiv \pm\mu \bmod p_2^{n-2}$; and this has a solution if $p_2$ is picked so that

$$\left(\frac{\pm\mu}{p_2^{n-2}}\right) = 1 \qquad \left(\text{where } \left(\frac{a}{b}\right) \text{ is the usual Jacobi symbol of } a \text{ and } b\right).$$

Hence

$$\operatorname{ord}\{nr^{n-1}[1 + (-1)^{n(n-1)/2} (n-1) s^2 d]^{-1}\} = 1$$

and

$$\operatorname{ord}\{(n-1) r^n[1 + (-1)^{n(n-1)/2} (n-1) s^2 d]^{-1}\} = 2.$$

Thus by Theorem 2.4 $f(x)$ has primitive Galois group.

THEOREM 2.6. *If a primitive permutation group contains a transposition, it is a symmetric group.*

*Proof.* See [16, p. 34].

The results of the following theorem are similar to the results obtained by Uchida [13] and Yamamoto [17]. The proof follows the lines of Yamamoto's [17, Proposition 2] except that we keep a more careful track of the choices of the coefficients $a$, $b$ so as to be able to fix the equivalence class of the discriminant.

THEOREM 2.7. *Let $k$ be an arbitrary algebraic number field, $d$ square-free in $k$, and $f(x) = x^n + ax + b \in k[x]$, $n \geqslant 3$, with splitting field $L$. Then $a$, $b$ can be chosen so that* $\operatorname{Gal}(L/k) \cong S_n$ *and* $D(f) = dm^2$, $m \in \mathcal{O}_k$.

*Proof.* By Lemma 2.1 we can take $a$, $b$ so that $D(f) = dm^2$. Now choose $r$, $s$ so that Lemmas 2.3 and 2.5 hold. Hence $f(x)$ has primitive

Galois group. Now by Theorem 2.6 it is enough to show that the Galois group of $f(x)$ contains a transposition. To do this we use the method of Van der Waerden [15, p. 190] and show that there exists $p_3(p_3')$ such that $f(x) \equiv g(x)\,h(x) \bmod p_3(p_3')$, where $g(x)$ is an irreducible polynomial of degree 2 and $h(x)$ is the product of $n-2$ distinct polynomials of degree 1.

Let $p$ be a prime number such that $p \equiv 1 \pmod 4$, $p \nmid n(n-1)$, and $p$ is unramified in $k$. Take $c, d_1 \in \mathbb{Z}$ so that $c^2 - 4d_1 = p$. Let

$$(*) \qquad 1/(1 + ct + d_1t^2) = 1 + e_1t + e_2t^2 + \cdots$$

be the formal expansion with respect to $t$; thus we have

$$\begin{aligned} &e_i \in \mathbb{Z} \quad \text{for} \quad i = 1, 2,\ldots, \\ &e_1 = -c, \\ &e_2 = -(ce_1 + d_1), \\ &e_i = -(ce_{i-1} + d_1e_{i-2}) \qquad \text{for} \quad i \geqslant 3. \end{aligned}$$

Let $g(x) = x^2 + cx + d_1$ and $h(x) = x^{n-2} + e_1x^{n-3} + \cdots + e_{n-2}$. Thus we have $g(x)\,h(x) = x^n - e_{n-1}x + d_1e_{n-2}$. Now we claim that $D(g)$ and $D(h)$ are relatively prime. Note that $D(g) = c^2 - 4d_1 = p$ and $D(gh) = D(g)\,D(h)\,R(g,h)^2$, where $R(g,h)$ is the resultant of $g$ and $h$. Thus it suffices to show that $\operatorname{ord}(D(gh)) = 1$. The equation $g(x) = 0$ gives a ramified quadratic extension $E_{\mathfrak{p}_i}$ over $k_{\mathfrak{p}_i}$, where $\mathfrak{p}_i \mid p$. Let $\alpha, \beta \in E_{\mathfrak{p}_i}^{\times}$ be the roots of $g(x)$; then we have $D(g) = (\alpha - \beta)^2 = c^2 - 4d_1 = p = \pi^2$ and $\pi = \alpha - \beta$ is a prime element of $E_{\mathfrak{p}_i}$.

In $E_{\mathfrak{p}_i}$ the expansion (*) now becomes

$$\frac{1}{1 + ct + d_1t^2} = \frac{1}{(1 - \alpha t)(1 - \beta t)} = \frac{1}{(\alpha - \beta)\,t}\left\{\frac{1}{1 - \alpha t} - \frac{1}{1 - \beta t}\right\}$$

$$= \frac{1}{(\alpha - \beta)} \sum_{k=0}^{\infty} (\alpha^{k+1} - \beta^{k+1})\,t^k.$$

Thus equating coefficients with (*) we have

$$e_k = \frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta} \qquad \text{for} \quad k = 1, 2,\ldots.$$

Replacing $\alpha$ by $\beta + \pi$ we have

$$\begin{aligned} e_k &= \left[\beta^{k+1} + (k+1)\,\pi\beta^k + \binom{k+1}{2}\pi^2\beta^{k-1}\right. \\ &\quad \left. + \binom{k+1}{3}\pi^3\beta^{k-2} + \cdots - \beta^{k+1}\right]\Big/\pi \\ &\equiv (k+1)\,\beta^k + \binom{k+1}{2}\pi\beta^{k-1} + \binom{k+1}{3}\pi^2\beta^{k-2} \pmod{\pi^3}. \end{aligned}$$

Applying the theorem of Swan,

$$
\begin{aligned}
D(gh) &= (-1)^{n(n-1)/2+n+1}\,(n-1)^{n-1}\,(-e_{n-1})^n \\
&\quad + (-1)^{n(n-1)/2}\,n^n(d_1e_{n-2})^{n-1} \\
&\equiv (-1)^{n(n-1)/2}\Big\{(-1)^{2n+1}\,(n-1)^{n-1} \\
&\quad \times \Big[n\beta^{n-1} + \binom{n}{2}\beta^{n-2}\pi + \binom{n}{3}\beta^{n-3}\pi^2\Big]^n \\
&\quad + n^n d_1^{n-1}\Big[(n-1)\,\beta^{n-2} + \binom{n-1}{2}\beta^{n-3}\pi \\
&\quad + \binom{n-1}{3}\beta^{n-4}\pi\Big]^{n-1}\Big\} \pmod{\pi^3} \\
&\equiv (-1)^{n(n-1)/2}\Big\{(-1)^{2n+1}\,(n-1)^{n-1} \\
&\quad \times \Big[n^n\beta^{n(n-1)} + \binom{n}{2}n^n\beta^{(n-1)^2+(n-2)}\pi \\
&\quad + \binom{n}{3}n^n\beta^{(n-1)^2+(n-3)}\pi^2 + \binom{n}{2}^3 n^{n-2}\beta^{(n-1)(n-2)+2n-4}\pi^2\Big] \\
&\quad + nd_1^{n-1}\Big[(n-1)^{n-1}\,\beta^{(n-2)(n-1)} \\
&\quad + \binom{n-1}{2}(n-1)^{n-1}\,\beta^{(n-2)^2+n-3}\pi \\
&\quad + \binom{n-1}{3}(n-1)^{n-1}\,\beta^{(n-2)^2+n-4}\pi^2 \\
&\quad + \binom{n-1}{2}^3 (n-1)^{n-3}\,\beta^{(n-2)(n-3)+2n-6}\pi^2\Big]\Big\} \pmod{\pi^3}.
\end{aligned}
$$

Now using the fact that $d_1 = \alpha\beta$ and $\alpha = \beta + \pi$, one finds that the coefficient of $\pi$ is zero and that the coefficient of $\pi^2$ is

$$(-1)^{(n-1)(n-2)/2}\,\tfrac{1}{8}n^{n+1}(n-1)^n\,\beta^{(n+1)(n-2)}.$$

Therefore

$$D(gh) \equiv (-1)^{(n-1)(n-2)/2}\,\tfrac{1}{8}n^{n+1}(n-1)^n\,\beta^{(n+1)(n-2)}\pi^2 \pmod{\pi^3}.$$

Since $p \nmid n(n-1)$, the coefficient of $\pi^2$ is a unit of $E_{\mathfrak{p}_i}$; thus $D(gh)$ is not divisible by $\pi^3$. Hence in $\mathcal{O}_k$ $D(gh) \in \mathfrak{p}_i$ for all $i$ but not in $\mathfrak{p}_i^2$ for all $i$

since $\pi^2 = p$. Because $D(g)$ and $D(h)$ are relatively prime, the splitting fields $K_g$ and $K_h$ of $g(x)$ and $h(x)$ over $k$ are linearly disjoint over $k$. From the Tchebotarev density theorem it follows that there exist infinitely many prime numbers that remain prime in $K_g$ but are decomposed completely in $K_h$. Let $p_3'$, $p_3$ be primes such that $p_3' \nmid p_1'p_2'D(gh)$ and $p_3 \nmid p_1p_2D(gh)$; then

$$f(x) \equiv g(x)\,h(x) \mod p_3' \qquad n \text{ odd},$$
$$f(x) \equiv g(x)\,h(x) \mod p_3 \qquad n \text{ even}.$$

Now take $r, s \in \mathcal{O}_k$ such that

$$(nr^{n-1} - (-1)^{n(n-1)/2}\,s^2d) \equiv -e_{n-1},$$
$$((n-1)\,rn^{-1})\,e_{n-1} \equiv d_1e_{n-2} \mod p_3'$$

or

$$nr^{n-1}/(1 + (-1)^{n(n-1)/2}\,(n-1)\,s^2d) \equiv -e_{n-1},$$
$$((n-1)\,rn^{-1})\,e_{n-1} \equiv -d_1e_{n-2} \mod p_3.$$

Thus for all $n \geqslant 3$ we have that an arbitrary quadratic number field is imbeddable in some $S_n$-extension.

COROLLARY 2.8. *Let $f(x)$ be as in Theorem* 2.7; *then there exist infinitely many $f(x)$ with Galois group isomorphic to $S_n$ and $D(f) = dm^2$.*

*Proof.* From the proof of Theorem 2.7 there are clearly an infinite number of $r$ and $s$ that satisfy the conditions in the proof of Theorem 2.7 in order for $f$ to have Galois group $S_n$.

EXAMPLES OF THEOREM 2.7.

(1) Let $n = 7, d = 3, p_1' = 11$ satisfy Lemma 2.3 with $r = 11r_1 + 1$, $s = 11s_1 \pm 4$. Lemma 2.5 is satisfied for $p_2' = 3$ with $r = 3 \cdot 11r_2 - 21$, $s = 3 \cdot 11s_2 \pm 4$ or $s = 3 \cdot 11s_2 \pm 7$. $p_3' = 19$ satisfies the conditions in the proof of Theorem 2.7 with $r = 3 \cdot 11 \cdot 19r_3 + 45$, $s = 3 \cdot 11 \cdot 19s_3 \pm 136$. Thus taking $r_3 = s_3 = 0$, $f(x)$ becomes

$$x^7 - (7 \cdot 45^6 + 3 \cdot 136^2)x - (6 \cdot 45/7)(7 \cdot 45^6 + 3 \cdot 136^2) = 0$$

or

$$x^7 - 58126414863 \cdot x - 15694132013010/7 = 0,$$

and

$$D(f) = 6^6(7 \cdot 45^6 + 3 \cdot 136^2)^6\,(3 \cdot 136^2)$$

and 3 does appear to an odd power in $D(f)$.

(2) Let $n = 8$, $d = 2$, $p_1 = 3$, $p_2 = 5$, and $p_3 = 11$; then $r = 3 \cdot 5 \cdot 11r_3 + 7$ and $s = 3 \cdot 5 \cdot 11s_3 - 157{,}564{,}391$. Thus taking $r_3 = s_3 = 0$, $f(x)$ becomes

$$x^8 + 8 \cdot 7^7 x/(1 + 2 \cdot 7 \cdot 157{,}564{,}391^2) + 7^9/(1 + 2 \cdot 7 \cdot 157{,}564{,}391^2) = 0$$

with

$$D(f) = (8/(1 + 2 \cdot 7 \cdot 157{,}564{,}391^2))^8 \cdot 7^{63} \cdot 2(1 + 7 \cdot 157{,}564{,}391^2),$$

and we note that 2 does appear to an odd power in $D(f)$.

We consider now the $A_n$-closure $K$ of $k$ and show how Theorem 2.7 "opens up" $K$.

THEOREM 2.9. *Let $K$ be the $A_n$-closure of $k$, $n \neq 4$; then $K$ has a $C_2$-extension $F$ and $F$ has an $A_n$-extension.*

*Proof.* Let $f(x) \in k[x]$ be as in Theorem 2.7. Now $f(x)$ is irreducible over $K$ since it is irreducible over $k$ and $A_n$ is the only normal subgroup of $S_n$. Hence taking $F = K(d^{1/2})$ we see that $F$ has an $A_n$-extension, the one belonging to $f(x)$.

## ACKNOWLEDGMENT

This work consists largely of the author's doctoral dissertation written at UCLA under the supervision of Professor Ernst Strauss, whom the author wishes to thank for his inspiration and guidance. The author is also grateful to Professors Basil Gordon and David Cantor for many helpful comments.

## REFERENCES

1. PH. FURTWÄNGLER, Über Kriterien für irreduzible und fur primitive Gleichungen und über die Aufstellung affektfreier Gleichungen, *Math. Ann.* **85** (1922), 34–40.
2. B. GORDON AND E. G. STRAUS, On the degrees of finite extensions of a field, *in* "Proceedings of Symposia in Pure Mathematics," Vol. VIII, American Mathematical Society, Providence, R.I., 1965.
3. M. HALL, "The Theory of Groups," Macmillan, New York, 1959.
4. D. HILBERT, Über die Irreduzibilität ganzer rationler Funktionen mit ganzzahligen Koeffizienten, *J. Reine Angew. Math.* **110** (1892), 104–129.
5. I. KAPLANSKY, "Fields and Rings," The Univ. of Chicago Press, Chicago, 1969.
6. D. KRAKOWSKI, Profinite groups and the Galois group of fields, Ph.D. Thesis, UCLA, 1971.
7. S. LANG, "Diophantine Geomentry," Interscience, New York, 1962.
8. P. MCCARTHY, "Algebraic Extensions of Fields," Blaisdall, Waltham, Mass., 1966.

9. I. R. ŠAFAREVIČ, Construction of fields of algebraic numbers with given solvable Galois groups, *Amer. Math. Soc. Transl. Ser. 2* **4** (1956), 185–237.
10. I. R. ŠAFAREVIČ, On the problem of imbedding fields, *Amer. Math. Soc. Transl. Ser. 2* **4** (1956), 151–183.
11. J. SONN, On the embedding problem for nonsolvable Galois groups of algebraic number fields: Reduction theorems, *J. Number Theory* **4** (1972), 411–436.
12. R. SWAN, Factorization of polynomials over finite fields, *Pacific J. Math.* **12** (1962), 1099–1106.
13. K. UCHIDA, Unramified extensions of quadratic number fields, II, *Tôhoku Math. J.* **22** (1970), 220–224.
14. J. V. USPENSKY, "Theory of Equations," McGraw–Hill, New York, 1948.
15. B. L. VAN DER WAERDEN, "Modern Algebra," Vol. I, Ungar, New York, 1953.
16. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.
17. Y. YAMAMOTO, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), 57–76.